PowerNet Global COMMUNICATIONS
100 Commercial Drive, Cincinnati, OH 45014
Phone: 513-942-7900, Fax: 513-942-5579
www.powernetglobal.com

March 4, 2008

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW, Suite TW-A325
Washington, DC 20554

Re: PNG Telecommunications, Inc.
EB Docket No. 06-36
Annual Certificate of Compliance for 2008

Dear Ms. Dortch:

Please find enclosed for filing in EB Docket No. 06-36 the certificate of PNG Telecommunications, Inc. required by 47 CFR § 64.2009(e) regarding its compliance with the Commissions rules concerning protection of Customer Proprietary Network Information.

Sincerely,

Dennis Packer

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date filed: March 4, 2008

Name of company covered by this certification: PNG Telecommunications, Inc.

Form 499 Filer ID: 003778289

Name of signatory: Dennis Packer

Title of signatory: General Counsel & Secretary

I, Dennis Packer, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI , and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed /s/ Dennis Packer

Statement of Procedures

The following briefly describes the procedures that PNG Telecommunications, Inc. ("PNG") has established to comply with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

1. Use of CPNI for Marketing

PNG does not use or disclose CPNI for marketing purposes.

2. Safeguards Against Unauthorized Disclosure

PNG's customers may access their account information, including CPNI, either through PNG's web portal or through a call to PNG's call center. Access to CPNI by either method requires the customer to provide the correct pre-established password. PNG requires that the password be a minimum of 8 characters and include at least one number and at least alpha character.

2.1 Access through Customer Web Portal

PNG Customers attempting to access their account via the customer web portal are prompted for their account number and the pre-established password. The customer is given three chances to enter the correct password. If the customer fails to enter the correct password on the third try, the account is locked and the customer is offered the chance to re-establish their password if they can correctly answer the backup security question which they established. When establishing the question, the customer has ten questions from which to choose, none of which are based on readily available biographical information (such of as account number, social security number or mother's maiden name). If the customer answers the backup security question correctly, they are led through a dialogue to re-establish their password. If the customer fails to answer the backup security question correctly, they are informed that PNG will contact them at the telephone number of record to re-establish their password.

2.2 Access through PNG's Call Center

PNG's Customer Service Representatives (CSRs) will not discuss or disclose CPNI with a person making an inbound call to PNG's Call Center until after the caller has given the correct pre-established password.

2.2.1 Establishment of Password

When a customer originally signs up for service with PNG, they are randomly assigned a temporary but unique 8 character code that is different from their account number. This code is transmitted to the customer in PNG's welcome letter or on the invoice. The welcome letter and invoice are mailed to the address given by the customer when they ordered service, that is, the address of record. If the customer calls the PNG Call Center and has not established a permanent password, the CSR asks the customer to read back the code on the welcome letter or invoice. If the customer reads the correct code to the CSR, the CSR leads the customer through the process of establishing a password and backup security question.

2.2.2 Subsequent Calls to the Call Center

If a customer who already has established a password and backup security question calls the Call Center, the CSR requests that the customer give their password at the beginning of the call. The customer gives the password and the CSR enters it into the system. The system then informs the CSR simply whether or not the customer gave the correct password. After the customer initially establishes their password and it is entered into the system, the password field is blanked on the CSR's screen.

If the customer fails to give the correct password after three attempts, the CSR gives the customer a chance to re-establish their password if the customer can correctly answer the backup security question. As with access via PNG's web portal, none of the backup security questions are based upon readily available biographical information. If the customer answers the backup security question correctly, the CSR leads the customer through the process of re-establishing a password. If the customer does not answer the backup security question correctly, then the CSR politely informs the customer that may not discuss the customer's account with the caller and that they will call them back at the telephone number of record and re-establish the password then.

2.3 Notice to Customers of Changes to their Account

If account information is changed, PNG notifies the customer that a change to the customer's account has occurred by sending an e-mail to the e-mail address of record. If no e-mail address of record exists, then PNG sends a letter by regular mail to the address of record. If the address of record has been changed within in the last 30 days, then PNG will call the telephone number of record.

3. Notice of Unauthorized Disclosure of or Access to CPNI

PNG has established procedures to notify law enforcement and customers according of unauthorized disclosure of or access to CPNI. PNG's director of network security and the manager of PNG's call center have been directed to report unauthorized disclosures and CPNI breaches to PNG's General Counsel. PNG's General Counsel then notifies law enforcement using the link provided on the Commission's web site and coordinates the notice to customers after the period for law enforcement objection to customer notice has passed.

4. Training & Discipline

PNG personnel, including but not limited to those in Customer Relations Management, Collections, Information Technology and Network, are trained in the these procedures and are disciplined according to PNG's standard disciplinary policies for failing to observe the established CPNI protection measures.

5. Summary

PNG believes that it has established rigorous procedures for the protection of CPNI. While PNG has not suffered a CPNI breach, PNG continues to monitor access to its CPNI and will modify its procedures as necessary in response to any such threat.